Module 3 | Reconnaissance & Vulnerability Identification

Introduction

In this module we're going to discuss initial recon and some of the tools used to do it. Reconnaissance is a vital part of system exploitation, for both attackers and defenders. Attackers need to gather information on a system of interest; defenders need to detect reconnaissance scans to prevent intrusion.

Things are getting a bit more complex and we're covering more content. We will build our testing lab and will start to conduct scanning both in that lab and against external targets.

Learning Objectives

The primary class objectives we address in this module is to *develop the ability to (1) design and execute and (2) defend against a malware campaign against a target* (Objective E). We also want to learn how *to scan systems and discover vulnerabilities* (Objective E.a), and how to *identify key information on organizations via public search engines and sources* (Objective E.b).

Notes: This module has one assignments at the end of the module. Please follow the submission guidelines to the letter.

All homework should be completed by the end of the third week.You'll use nmap and Kali Linux (http://www.kali.org) in the assignment at the end of this module. Nmap is installed with Kali Linux. You'll use these tools to scan and analyze a virtual machine in a virtual laboratory you'll build while following the lectures and then prepare a report covering your findings.

Required Instructional Materials

All you'll need for this section are the video lectures and the tooling we cover. You'll need an internet connection to access, install, and read about the tools we discuss.

Summary

- This module consists of a series of video lectures. We reference a variety of tools and external sites and documentation you'll likely want to review. The links you need will be included in the slides.
- We have a homework assignment that will be graded at the end of this module.